DETAILED ACTION

1. Claims 1-5, 7-13, 15-20 and 22-26 are pending in this application.

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 08,2009 has been entered.

Examiner's Amendment

An Examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to the Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephonic interview with Sabra-Anne Truesdale on 03/09/2009.

The application has been amended as follows:

1. (Currently Amended) A network security system comprising:

a first distributed software agent comprising a processor configured to collect a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;

a second distributed software agent comprising a processor configured to collect a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock; and

a manager module in communication with the distributed software agents, the manager module comprising a processor configured to:

receive the first and second stream of alerts;

identify a first alert in the first stream and a second alert in the second stream,

wherein the first alert includes an Internet Protocol (IP) address, and

wherein the second alert includes the IP address;

determine, based on the first alert and the second alert, whether the first clock

and the second clock are synchronized; and

[[if]] when the first clock and the second clock are not synchronized:

synchronize the first clock and the second clock;

modify at least one of a timestamp within the first alert and a timestamp within the second alert; and

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

9. (Currently Amended) A method performed by a network security system, the method comprising:

receiving a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;

receiving a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time

of detection by the second network security device according to the second clock;

identifying a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address;

determining, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and

[[if]] when the first clock and the second clock are not synchronized:

synchronizing the first clock and the second clock;

modifying at least one of a timestamp within the first alert and a timestamp within the second alert; and

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determining whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

16. (Currently Amended) A machine readable medium storing a set of instructions that, when executed by the machine, cause the machine to:

receive a first stream of alerts from a first network security device having a first clock, each alert in the first stream representing an event detected by the first network security device and including a time of detection by the first network security device according to the first clock;

receive a second stream of alerts from a second network security device having a second clock, each alert in the second stream representing an event detected by the second network security device and including a time of detection by the second network security device according to the second clock;

identify a first alert in the first stream and a second alert in the second stream wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address;

determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and

[[if]] when the first clock and the second clock are not synchronized:

synchronize the first clock and the second clock;

modify at least one of a timestamp within the first alert and a timestamp within the second alert; and

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

23. (Currently Amended) A network security system comprising:

a plurality of distributed software agents, each comprising a processor configured

to collect alerts from a plurality of corresponding network security devices, each network security device having a clock; and

a manager module in communication with the distributed software agents, the manager module comprising a processor configured to:

receive the alerts;

identify alerts from a subset of the plurality of network security devices, wherein all of the identified alerts include a particular Internet Protocol (IP) address;

determine, based on the identified alerts, whether the clocks of the subset of the plurality of network security devices are synchronized; and

[[if]] when the clocks of the subset of the plurality of network security devices are not synchronized:

synchronize the clocks of the subset of the plurality of network security devices;

modify at least one of a timestamp within a first identified alert and a timestamp within a second identified alert; and

after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred.

Allowable Subject Matter

2. The following is an Examiner's statement of reasons for allowance: Claims 1-5, 7-13, 15-20 and 22-26 are allowed.

3. The Examiner had found that the prior art of record does not teach or suggest or render obvious "The following is an Examiner's statement of reasons for allowance: "a manager module in communication with the distributed software agents, the manager module comprising a processor configured to: receive the first and second stream of alerts; identify a first alert in the first stream and a second alert in the second stream, wherein the first alert includes an Internet Protocol (IP) address, and wherein the second alert includes the IP address; determine, based on the first alert and the second alert, whether the first clock and the second clock are synchronized; and when the first clock and the second clock are not synchronized: synchronize the first clock and the second clock; modify at least one of a timestamp within the first alert and a timestamp within the second alert; and after having modified at least one of the timestamp within the first alert and the timestamp within the second alert, determine whether the first alert and the second alert satisfy a condition of a rule, wherein the rule determines whether a security incident has occurred" as in claims 1, 9, 16 and 23.

4. Any comments considered necessary by the Applicant must by submitted no later than the payment of the issue fee and, to avoid processing delays, should

preferable accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance or Examiner Amendment."

Conclusion

5. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SUMAN DEBNATH whose telephone number is (571)270-1256. The examiner can normally be reached on 8 am to 5 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. D./
Examiner, Art Unit 2435
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435